Information

zu den

Datenverarbeitungen iSd

EU Datenschutz-Grundverordnung (DSGVO)

Version von 2019-04-06

Inhaltsverzeichnis

Kapitel 1

Vorbemerkungen

Am 25. Mai 2018 wurde das Datenschutzgesetz 2000 (DSG 2000) durch die EU-DSGVO (Datenschutz-Grundverordnung) abgelöst. Als EU-Verordnung ist diese unmittelbar - d.h. ohne Umsetzung in nationales Recht - anzuwenden. Die Rechtmäßigkeit der Verarbeitung nach den Bestimmungen des DSG 2000 ergab sich u.a. aus den Standardanwendungen, die in der Liste, im Anhang 1 der StMV (Standard- und Muster-Verordnung), aufgelistet sind.

Die Artikelbezeichnungen beziehen sich - wenn nichts anderes vermerkt ist - auf die DSGVO. Verweise auf das Bilanzbuchhaltungsberufegesetzt (BiBuG) 2014 beziehen sich auf die Fassung des BGBl. I 32 / 2018.

BiBuG-Berufsberechtigte unterliegen nach den Bestimmungen des § 39 BiBuG einer strengen Verschwiegenheitsverpflichtung, die auch nach dem Ende des Auftragsverhältnisses mit dem Kunden weitergilt. Diese Verschwiegenheitspflicht löst in anderen Materiegesetzen ein Zeugnisentschlagungsrecht aus, wobei dieses iSd § 39 BiBuG als Pflicht zu verstehen ist.

Die Berufsrechte dürfen erst nach der öffentlichen Bestellung durch die Aufsichtsbehörde ausgeübt werden (§§ 6 ff BiBuG).

Kapitel 2

Informationen

2.1 Art. 4

Nach der Legaldefinition der Z. 7 entscheidet ein Verantwortlicher über die Mittel und Zwecke der Datenverarbeitung alleine oder gemeinsam mit einem anderen Verantwortlichen.

§ 33 Abs. 1 BiBuG verpflichtet Berufsberechtigte Ihren Beruf gewissenhaft, sorgfältig, eigenverantwortlich und unabhängig auszuüben.

§ 36 Abs. 1 BiBuG verpflichtet Berufsberechtigte Aufträge abzulehnen, bei denen sie an fachliche Weisungen des Auftraggebers gebunden wären. § 4 Abs. 4 der Berufsausübungsrichtlinie (BB-AR 2014) verlangt die Zurücklegung eines Auftrages, wenn sich nachträglich die Unerfüllbarkeit des verlangten Verhaltens herausstellen sollte.

Da ein Auftragsverarbeiter (iSd Legaldefinition der Z. 8) gemäß Art. 28 Abs. 3 Z. a nur bei Vorliegen einer dokumentierten Weisung des auftraggebenden Verantwortlichen eine Datenverarbeitung durchführen darf, kommt für die BhB KG nur die Einstufung als Verantwortlicher iSd der Legaldefinition der Z. 7 in Frage.

2.2 Art. 5

Artikel 5 hat die Überschrift "Grundsätze für die Verarbeitung personenbezogener Daten". Auf die genannten Grundsätze

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glaube
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit

- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

wird, soweit nötig, im Folgenden eingegangen.

2.2.1 Speicherbegrenzung

Berufsberechtigte haben insbesonders gemäß den nachfolgenden gesetzlichen Bestimmungen die verarbeiteten Daten aufzubewahren:

- gemäß § 132 BAO für die Dauern von 7 Jahren - die Frist beginnt mit Ablauf des Kalenderjahres zu laufen;
- gemäß § 207 BAO für eine Dauer von 10 Jahren ab dem Ende des Kalenderjahres in dem die Abgabenverkürzung beendet wurde. Mit § 209 BAO verlängert sich diese Frist, wenn nach außen erkennbare Amtshandlungen zur Geltendmachung unternommen werden, um deren Dauer;
- gemäß § 11 Abs. 2 UStG letzter Satz für die Dauer von 7 Jahren;
- gemäß § 18 Abs. 10 UStG für eine Dauer von 22 Jahren (bei Grundstücksumsätzen);
- gemäß § 212 UGB für eine Dauer von 7 ab dem Ende des Kalenderjahres;
- gemäß § 41a ASVG kommen die Aufbewahrungsfristen der BAO zur Anwendung;
- gemäß Gleichbehandlungsgesetz für eine Dauer von 7 Monaten, für die mögliche Abwehr eines Schadenersatzbegehrens wegen (behaupteter) Diskriminierung.

Während einer Außenprüfung nach den Bestimmungen der §§ 147 ff BAO ist der Fristenlauf gehemmt. Ebenso während der Ausschöpfung von Rechtsmitteln gegen ergangene Bescheide iSd § 92 BAO.

Die Frist zum Ablauf der Aufbewahrungspflicht wird auch gehemmt, solange ein behördliches oder gerichtliches Verfahren droht oder bereits anhängig ist, in dem die verarbeiteten Daten benötigt werden könnten.

Wie lange die Daten zu speichern sind, ist daher eine Einzelfallentscheidung, die von der Gesamtheit der Umstände abhängig sind. Diese Entscheidung kann nur ex ante getroffen werden.

2.3 Art. 6

Die "Rechtmäßigkeit der Verarbeitung" der zu verarbeitenden Daten iSd Abs. 1 lit. a bis f ergibt sich einerseits durch den erteilten Auftrag vom Kunden und andererseits durch rechtliche Vorgaben. Diese ergeben sich vor allem aus Pflichten zum Führen von Aufzeichnungen, die im Abgabenrecht, im Arbeitsrecht sowie im Sozialversicherungsrecht definiert sind.

Durch die Begründung eines Vertragsverhältnisses mit einem Kunden, sind dessen persönliche Daten, als abgabenpflichtige Person, zu verarbeiten (lit. a).

Lit. b kommt zur Anwendung, wenn vor Vertragsabschluß zu prüfen ist, ob in Bezug auf die Bestimmungen der EU-Richtlinie zur Vermeidung von Geldwäsche und Terrorismusfinanzierung[1] die vereinfachte Prüfung angewandt werden darf, oder ob die erhöhten Sorgfaltspflichten anzuwenden sind. Siehe auch [2].

Die lit. c, e und f werden über die bereits oben erwähnten rechtlichen Pflichten, Daten für die Zwecke der Abgabenerhebung zu erfassen, erfüllt. Zusätzlich kommen die Verpflichtungen zur Archivierung der Daten - neben den im Kapitel 2.2.1 genannten - noch beispielsweise folgenden Bestimmungen zur Anwendung: § 8 ArbIG, § 5 ASchG und § 26 AZG

Für das Sozialversicherungsrecht seien exemplarisch die §§ 33 ff ASVG angeführt. Damit werden die Grundsätze der *Rechtmäßigkeit* und der *Zweckbindung* des. Art. 5 erreicht.

Der gesetzliche Auftrag zur Verarbeitung von (personenbezogenen) Daten - iSd lit. e - hat starken Einfluß auf die Erfüllung der Art. 33 ff. Das öffentliche Interesse der lit. e besteht beispielsweise in der gleichmäßigen Einhebung der Abgaben iSd § 114 Abs. 1 BAO.

2.4 Art. 9

Die "Verarbeitung besonderer Kategorien personenbezogener Daten" meint die sensiblen Daten iSd DSG 2000.

Auch bisher wurden keine Daten verarbeitet, aus denen die rassische oder ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit ableitbar sind. Dies entspricht dem Grundsatz der *Datenminimierung* des Art. 5. Derartige Daten werden auch weiterhin nicht verarbeitet werden können, da es in den Speicherstrukturen nicht vorgesehen ist, derartige besondere Kategorien, zu speichern - in Übereinstimmung mit dem Grundsatz der *Speicherbegrenzung* des Art. 5.

Die Ausnahmen nach Abs. 2 lit. b bzw. lit. g, die eine Verarbeitung besonderer Kategorien erlauben, beziehen sich exemplarisch auf die Erfüllung des Abgabenrechtes oder auf arbeitsrechtliche Bestimmungen wie z.B. die Entgeltfortzahlung im Krankheitsfall. Für das Abgabenrecht sei exemplarisch die gesetzlich normierte Führung des Lohnkontos erwähnt.

[1] siehe Art. 41 und Art. 43 der RL 849/2015/EU

2.5 Art. 13

Die "Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person" darf gem. Abs. 4 entfallen, wenn diese Information bereits bei der betroffenen Person vorhanden ist.

§ 2 ABGB definiert das "Wissen müssen" im österreichischen Rechtsbestand. Von Unternehmern (=Steuerpflichtiger) wird generell verlangt, sich über die einzuhaltende Rechtsmaterie zu erkundigen. Von jedem Dienstnehmer werden persönliche Daten für die Ausstellung des Dienstvertrages und für die Einhaltung der Meldepflichten der §§ 33 ff ASVG verlangt. Somit darf das Vorhandensein dieser Informationen angenommen werden und eine gesonderte Informationspflicht entfällt.

2.6 Art. 14

Die "Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden" betrifft zum einen nur Dienstnehmer des Kunden. Zum anderen entfällt gem. 5 diese Pflicht, wenn (lit. a) die betroffene Person bereits über die Information verfügt, oder (lit. d) die zu verarbeitenden Daten einem Berufsgeheimnis unterliegen und daher vertraulich zu behandeln sind.

§ 39 BiBuG verpflichtet jeden Berufsberechtigten zur Verschwiegenheit, die nach dem Ende des Vertragsverhältnisses fortdauert. Somit kann unter Anwendung des Abs. 5 lit. d diese zusätzliche Informationspflicht entfallen. Lit. a wäre erfüllt, wenn diese Information vom Kunden an seine Dienstnehmer erteilt wird.

Mit der Verschwiegenheitspflicht des § 39 BiBuG wird der Grundsatz der *Vertraulichkeit* des Art. 5 erfüllt.

2.7 Art. 17

Das "Recht auf Löschung" gilt nicht wenn Abs. 3 lit. b oder Abs. 3 lit. e zutrifft. Beide Bedinungen sind durch die Darstellung im Kapitel 2.2.1 zutreffend.

Technisch bedingt ist ein nach Abs. 1 zulässiges Löschen von Daten, die sich in einer Sicherungen befinden, die gemäß Art. 32 Abs. 1 lit. c (siehe Kapitel 2.12.1) anzulegen sind, nicht möglich. Hierzu sei auf Kapitel 2.8.1 verwiesen.

2.8 Art. 18

Die Beschränkung des "Recht auf Einschränkung der Verarbeitung" nach Abs. 2 ist nötig, um der Verpflichtung auf rasche Wiederherstellung bei einem Zwischenfall (siehe Kapitel 2.12.1) nachkommen zu können.

2.8.1 Abs. 2

In Anwendung des § 4 Abs. 2 DSG 2018 werden Daten, für die die Löschung nach Art. 17 Abs. 1 zulässig ist, durch deren Überschreiben im Rahmen des Backup-Konzeptes (siehe Kapitel 2.12.1), gelöscht. Die Einschränkung der Verarbeitung ergibt sich aus der Tatsache, daß ein Sicherungsmedium (organisatorisch) der regulären Verarbeitung entzogen ist.

2.9 Art. 24

Die "Verantwortung des für die Verarbeitung Verantwortlichen" umfaßt u.a. die beim Art. 25 beschriebenen technischen Maßnahmen bzw. die beim Art. 32 beschriebenen organisatorischen Maßnahmen.

2.10 Art. 25

Der "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" wird - obwohl im Prinzip untrennbar, da beides einander bedingt - hier getrennt behandelt. Die weiterführenden Details, sowie die Ergebnisse der Risikoanlayse, sind als Betriebs- und Geschäftsgeheimnisse klassifiziert, und daher an anderer Stelle dokumentiert.

2.10.1 Security by Design

Zum Datenschutz durch Technikgestaltung gehört u.a. die Verwendung einer privaten Netzwerkadresse[2] für das Intranet. Zugriffe über das Internet - z.B. durch einen VPN-Tunnel - sind weder vorhanden noch geplant. Meldungen wie z.B. [6] sind eine (nachträgliche) Bestätigung für diese Designentscheidung. Die Verwendung von WLAN war schon vor dem Bekanntwerden der "KRACK-Attacke[3]" nicht möglich. Trotz der Beschreibung in [5] wird es dabei bleiben.

2.10.2 Security by Default

Zum Datenschutz durch datenschutzfreundliche Voreinstellungen muß festgehalten werden, daß Microsoft Produkte "insecure by default" sind. Deswegen kommen - wo möglich - nur mehr Open Source Produkte zum Einsatz[4]. Durch legistische Maßnahmen, wie z.B. den US Patriot Act, der US Behörden vollen Zugriff auf alle Daten gewährt, die sich in einer "Cloud" befinden, wenn der Betreiber ein amerikanisches Unternehmen ist oder einen amerikanischen Eigentümer hat, verbietet den Einsatz jeder Art von Cloud-Lösung von selbst.

Aus der langjährigen Erfahrung mit Microsoft-Produkten[5] sei empfohlen *nicht* auf Windows 10 zu migrieren, sondern bei Windows 7 oder Windows 8 zu bleiben.

[2] RFC 1918
[3] Siehe 4.
[4] Für die Open Source Community hat Datensicherheit eine sehr hohe Priorität.
[5] von DOS 3.2 bis inklusive Windows 10.

Die Microsoft-Konfiguration von Windows 10 gewährt vom Werk aus, jeder MS App den Vollzugriff auf alle Daten - inklusive aktivierter Geo-Location, aktivierter Kamera-App und aktivierter Mikrofon-App. Während es bei Windows 7 noch vergleichsweise einfach war, die Konfiguration zu finden, um eine datenschutzfreundlichere Einstellung vornehmen zu können, wird mittlerweile bei Windows 10 diese Konfiguration so gut versteckt, daß man explizit wissen muß, mit welchem aufzurufenden Tool eine datenschutzfreundlichere Einstellung erreicht werden kann. Bei Windows 8 sind diese Einstellungen bereits besser versteckt als noch bei Windows 7, aber leichter erreichbar als bei Windows 10.

2.11 Art. 30

Der für die Datenverarbeitung Verantwortliche ist der Komplementär der Buchhaltung Blaschka KG. Der Name und die Kontaktdaten können entweder dem öffentlich einsehbaren Firmenbuch entnommen werden, oder dem Impressum[6]. Mitarbeiter und gegebenenfalls Auftragnehmer unterliegen der Verschwiegenheitspflicht des § 39 BiBuG. Das Verzeichnis selbst ist ein eigenständiges Dokument - siehe [1].

2.12 Art. 32

Die "Sicherheit der Verarbeitung" soll durch ein Bündel an Maßnahmen erreicht werden. Dazu gehören u.a. die Verwendung einer privaten Netzwerkadresse[7], ein Backup-Konzept (Abs. 1 lit. c) und organisatorische Maßnahmen (Abs. 4). Zu den organisatorischen Maßnahmen gehört u.a. die Verpflichtungserklärung der Dienstnehmer[8], und speziell die Schaffung von Risikobewußtsein, um beispielsweise nicht jede Mail "blind" zu öffnen. Die Details zum Abs. 1 lit. b sind als Betriebs- und Geschäftsgeheimnis klassifiziert und an anderer Stelle dokumentiert.

Aus der Auswertung der anfallenden Daten ist bekannt, daß am SSH-Port in jeder Sekunde bis zu drei parallele Angriffe stattfinden. Beim Mail-Sub-System (Port 25) kommt es im Durchschnitt alle 15 Sekunden zu einem Versuch, die Sicherheitsmaßnahmen auszuhebeln. ftp (Port 21) wird mehrmals am Tag mit "Bulk Angriffen" konfrontiert. Der Web-Server liefert jeden Tag rd. 500 MB an Datenvolumen aus. Durch den konsequenten Einsatz von sicherheitsbewußten Open Source-Produkten und der entsprechenden Konfiguration konnte noch kein gelungener Einbruchsversuch festgestellt werden.

2.12.1 Abs. 1 lit. c

Die verlangte Fähigkeit bei einem physischen oder technischen Zwischenfall die Daten rasch wiederherstellen zu können, ist die Forderung ein Backup- bzw. Sicherungskonzept für die verarbeiteten Daten einzurichten und zu pflegen. Wobei

[6] Siehe 3.
[7] iSd Internet Standard RFC 1918
[8] § 39 Abs. 5 BiBuG idgF

diese Bestimmung den Grundsatz der Speicherminimierung im Art. 5 (siehe Kapitel 2.2.1) materiell derogiert.

Die konkrete Ausgestaltung des Datensicherungskonzeptes ist als Betriebs- und Geschäftsgeheimnis klassifiziert und an anderer Stelle dokumentiert.

2.13 Art. 33

Die "Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde" wird voraussichtlich unterbleiben können, da nur solche Daten verarbeitet werden, für die es einen gesetzlichen Auftrag gibt. Daher wird es voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führen, wenn eine Datenschutzverletzung festgestellt wird.

Sollte eine Verletzung des Datenschutzes festgestellt werden, wird im Einzelfall zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet, kann eine Meldung an die Aufsichtsbehörde zu erstatten sein.

2.14 Art. 34

Die "Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" wird mit hoher Wahrscheinlichkeit nicht nötig werden, da diese Meldung ein **hohes** Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen als Voraussetzung hat.

Da die Datenverarbeitung auf gesetzlichen Vorgaben basiert, ist es auch nicht möglich, durch diese Datenverarbeitung, in Rechte oder Freiheiten von natürlichen Personen einzugreifen, da dies bereits durch den Gesetzgeber erfolgt ist, der die Verarbeitung der Daten angeordnet hat.

Sollte eine Verletzung des Datenschutzes festgestellt werden, wird im Einzelfall zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet, kann eine Meldung an betroffene natürliche Personen zu erstatten sein.

2.15 Art. 35

Die "Datenschutz-Folgenabschätzung" ist durchzuführen, wenn die Datenverarbeitung **voraussichtlich** ein **hohes** Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung[9] (DSFA-AV) nimmt alle in Anwendung befindlichen Datenverarbeitungen von der Durchführung einer Datenschutz-Folgenabschätzung aus.

[9] BGBl. II 108 / 2018

2.16 Art. 37

Die ”Benennung eines Datenschutzbeauftragten” ist nach Abs. 1 nicht nötig. Die BhB KG ist weder eine Behörde (lit. a), noch gehört es zur Kerntätigkeit eine regelmäßige bzw. systematische Überwachung von betroffenen Personen durchzuführen (lit. b). Ebensowenig gehört die umfangreiche Verarbeitung besonderer Kategorien (iSv sensibler Daten) von Daten zur Kerntätigkeit (lit. c).

Auf das Recht, nach Abs. 2, freiwillig einen Datenschutzbeauftragten zu ernennen, wird verzichtet. Somit entfällt auch die Mitteilungspflicht nach Abs. 7.

Literatur

[1] Buchhaltung Blaschka KG. *Datenverarbeitungsregister iSd Art. 30 Abs. 1 DSGVO*. 2018.

[2] Buchhaltung Blaschka KG. *Dokumentation zu den berufsrechtlichen Vorgaben durch die 4. EU-Geldwäsche-RL*. 2019.

[3] Buchhaltung Blaschka KG. *Impressum*. URL: https://www.buchhaltung-blaschka.at/Impressum.html.

[4] *KRACK Angriff auf WPA2 (1)*. URL: https://www.heise.de/security/meldung/Details-zur-KRACK-Attacke-WPA2-ist-angeschlagen-aber-nicht-gaenzlich-geknackt-3862571.html (besucht am 17. 10. 2017).

[5] *KRACK Angriff auf WPA2 (2)*. URL: https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html (besucht am 20. 10. 2017).

[6] *KRACK-Attacke*. URL: https://www.heise.de/newsticker/meldung/Linus-Torvalds-Will-Intel-Scheisse-fuer-immer-und-ewig-verkaufen-3934829.html (besucht am 17. 10. 2017).

Versionshistorie

Ver.	Gültig ab	Änderung(en)
1.0	2019-04-06	Initialversion durch Abspaltung.